(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－50422

(43)公開日　平成9年（1997）2月18日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０	Ａ
	12/00	５４７	7623－5B		12/00	５４７	Ｈ
	13/00	３５１	9460－5E		13/00	３５１	Ａ
		３５５	9460－5E			３５５	

審査請求　未請求　請求項の数２　ＯＬ（全 9 頁）

(21)出願番号　特願平7－200107

(22)出願日　平成7年（1995）8月4日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者　斉藤　典明
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(72)発明者　水澤　純一
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

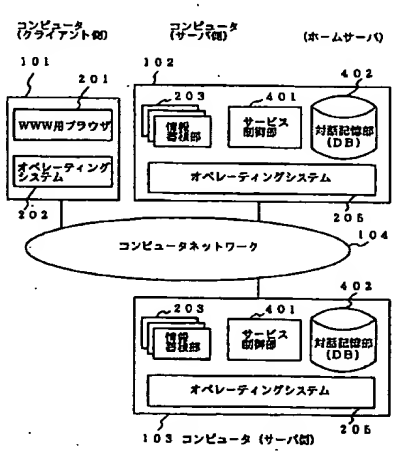
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】コンピュータネットワーク上の対話継承型アクセス制御方法及びそのサーバコンピュータ

(57)【要約】

【課題】　コンピュータネットワーク上の複数サーバをまたがった一連のアクセスにおいて、一貫性を持ったアクセス制御を可能にする。

【解決手段】　クライアント１０１とサーバ１０２，１０３はネットワーク１０４によって接続される。１０２は１０１を用いているユーザのユーザ情報を管理しているホームサーバであり、１０３は１０１のユーザ情報を管理していないサーバである。１０１はユーザからのＵＲＬに従い、１０２や１０３に情報取得要求を発行する。１０２や１０３は情報取得要求中の対話ＩＤを解析し、同一ユーザの識別、一連のアクセスの記憶、アクセスのチェックを行う。そして、必要なら他のサーバへ問い合わせて、他のサーバ発行の対話ＩＤも有効にする。



1

【特許請求の範囲】

【請求項1】　情報提供用のWorld-Wide Webを有するサーバコンピュータとWorld-Wide Webからの情報取得のためのブラウザを有するクライアントコンピュータを含むコンピュータネットワークにおけるサーバ側のアクセス制御方法であって、

クライアント側からの情報取得要求受信時、初回の情報取得要求か、第2回目以降の情報取得要求かを判定し、初回の情報取得の場合は、ＩＤ取得要求付き情報要求をもつ初期画面のハイパーテキストをクライアント側に返送し、

第2回目以降の情報取得要求の時、ＩＤの取得要求があり情報提供条件を満たしたユーザからの要求であった場合には、発行元サーバの明記された対話ＩＤを生成し、該対話ＩＤを対話記憶部に登録し、該対話ＩＤを付加したハイパーテキストをクライアントに側に返送し、

ＩＤ取得要求でない情報取得要求の場合は、情報取得要求内の対話ＩＤを抽出し、該対話ＩＤから判明する発行元サーバに問い合わせを行い、該発行元サーバからのユーザ認証の結果に基づき情報提供の可否の判定を行い、対話ＩＤが存在しない場合、または正規の対話ＩＤでない場合、または、正規の対話ＩＤでもユーザの属性により情報提供を認めない場合には、アクセス拒否を行うことを特徴とするコンピュータネットワーク上の対話継承型アクセス制御方法。

【請求項2】　コンピュータネットワークで接続したクライアントコンピュータに対し、World-Wide Webの情報をHyper Transfer Protocolにより提供するサーバコンピュータにおいて、

同一ユーザからの一連のアクセスを識別する対話識別手段と、同一ユーザのアクセスの履歴を記憶する対話記憶手段と、アクセス履歴を複数サーバから参照する事により情報提供を制御する制御手段を有することを特徴とするサーバコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワーク上の対話継承型アクセス制御方法及びそのサーバコンピュータに関し、詳しくは、ハイパーテキストをコンピュータネットワーク上でユーザに提供するための通信サービスのアクセス制御に関するものである。

【０００２】

【従来の技術】従来、ハイパーテキストをコンピュータネットワーク上で、ユーザに対して提供する通信サービスとしてWWW（World-Wide Web）が知られており、そのための方法としてＨＴＴＰ（Hyper Text Transfer Protocol）がある。この方法は、不特定多数のユーザへのサービス提供を行うものであるが、従来はユーザのハイパーテキストに対する一連の操作に対して情報取得の要求が生じた時のみ、情報取得要求中のプロトコル、ＩＰアドレス（サーバアドレス）、ポート番号、取得する情報等を設定したＵＲＬ（Uniform Resource Locator）で指定されるサービス提供元のサーバに接続を行い情報の取得を行っている。

2

【０００３】図7は、この従来のWWWのシステム構成を示したものである。同図において、１０１はサービスの提供を受けるためにユーザが用いるコンピュータ（クライアント側コンピュータ）、１０３はサービスを提供するためのコンピュータ（サーバ側コンピュータ）で、両者はネットワーク１０４によって接続されている。コンピュータ１０１の内部において、２０１がWWWサービスの提供を受けるための各種ブラウザ、２０２が該コンピュータ１０１を制御するための各種オペレーティングシステムであり、また、コンピュータ１０３の内部において、２０３がWWWサービスにおいてユーザに提供するための情報（ハイパーテキストなど）の蓄積部、２０４がWWWサービスを提供するための各種デーモン、２０５が該コンピュータ１０３を制御するための各種オペレーティングシステムである。ブラウザ２０１では、コンピュータの入力装置から入力されたユーザからのＵＲＬに従い、ネットワーク上のWWWサーバに情報取得要求を発行する。情報取得要求を受けたWWWサーバのデーモン２０４では、ＵＲＬで示される情報蓄積部２０３内の情報をユーザに転送する。

【０００４】図8に、この従来のWWWサーバのサービス提供シーケンスの一例を示す。同図において、複数のユーザから複数回情報提供要求がある場合でも同様の手順で情報を返送する。

【０００５】上記従来のWWWにおけるＨＴＴＰは、不特定多数のユーザへの通信サービスが対象であり、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴により情報の保護が行えない。

【０００６】これに対して、先に本出願人は、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴による情報の保護を行う機能を拡張した方式を提案した（特願平７－１２５３８７号「対話管理型情報提供方法及び装置」）。

【０００７】図9は、特願平７－１２５３８７号のシステム構成を示したものである。１０１，１０３及び１０４は図7と同様である。クライアント側コンピュータ１０１の内部において、２０１がWWWサービスの提供を受けるための各種ブラウザ、２０２が該コンピュータ１０１を制御するための各種オペレーティングシステムであり、また、サーバ側コンピュータ１０３の内部において、２０３がWWWサービスにおいてユーザに提供するための情報（ハイパーテキストなど）の蓄積部、４０１が対話管理可能なWWWサービスを提供するためのデーモン、４０２が対話管理を行うために必要な情報を蓄積する対話記憶部、２０５が該コンピュータを制御するた

めの各種オペレーティングシステムである。ブラウザ２０１からは、コンピュータの入力装置から入力されたユーザからのＵＲＬに従い、ネットワーク上のWWWサーバに情報取得要求が発行される。情報取得要求を受けたWWWサーバのデーモン４０１では、対話記憶部４０２の情報をもとにWWWサービスの提供の可否を判定し、サービス提供を許可する場合にはＵＲＬで示される情報蓄積部２０３内の情報をユーザに転送する。

【０００８】図１０に、この場合のクライアントとサーバ間のシーケンスの一例を示す。ここで、一連のアクセスを対話と呼ぶことにする。ユーザからのアクセスの初期の段階において、サーバがその対話に対する識別子（対話ＩＤ）を生成し、次回のアクセスに必要となるＵＲＬにその対話ＩＤを付加したハイパーテキストをユーザに提供する。クライアントからは、転送されてきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話ＩＤ付きＵＲＬによってサーバにアクセスを行う。

【０００９】上記特願平７－１２５３８７号の方式では、不特定多数のユーザを対象とした通信サービスにおいて高度がアクセス制御が可能であるが、これらの機能の有効範囲はそれぞれの情報提供元のサーバに対してのみである。このため、WWWを用いた一連の情報取得において、コンピュータネットワーク上の様々な情報提供サーバ間をまたがってアクセスする場合、それぞれのサーバにおいて別々に情報取得要求の認証を行う必要が生じる。

【００１０】

【発明が解決しようとする課題】本発明の目的は、ハイパーテキストをコンピュータネットワーク上で、不特定多数のユーザに提供するWWWを用いた通信サービスにおいて、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴による情報の保護等の高度なアクセス制御を可能にすると同時に、複数のサーバをまたがった一連のアクセスにおいても一貫性を持ったアクセス制御を可能にして、それぞれのサーバでの別々の情報取得要求の認証を不要にすることにある。

【００１１】

【課題を解決するための手段】本発明は、WWWにおけるＨＴＴＰで利用されるＵＲＬに先の特願平７－１２５３８７号で導入した同一ユーザからの一連の情報を識別する識別子（対話ＩＤ）を、コンピュータネットワーク上に多数存在するサーバ間で継承して管理する事を最も主要な特徴とする。

【００１２】

【作用】本発明では、ユーザからのアクセスの初期の段階において、サーバがその対話に対する識別子（対話ＩＤ）を生成し、次回のアクセスに必要となるＵＲＬと対話ＩＤを付加したハイパーテキストをユーザに提供する。クライアントからは、転送されてきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話ＩＤとＵＲＬによってサーバにアクセスを行う。サーバはクライアントから送信されたきた情報取得要求の中の対話ＩＤを解析し、同一ユーザの識別、一連のアクセスの記憶、所定のアクセスのチェックなどを行う。これらのチェックにおいて、自サーバ内の対話ＩＤの管理情報による識別だけでなく、他のサーバで管理されている対話ＩＤについても該当のサーバへの問合わせを行い、他のサーバ発行の対話ＩＤも有効にする。これにより、サーバをまたがった一連のアクセスにおいても、一貫性を持ったアクセス制御ができるようになる。

【００１３】

【実施例】以下、本発明について図面を参照して説明する。

【００１４】図１は、本発明を適用するコンピュータネットワークの一実施例を示したものである。同図において、１０１はサービスの提供を受けるためにユーザが用いるコンピュータ（クライアント側コンピュータ）、１０２および１０３はサービスを提供するためのコンピュータ（サーバ側コンピュータ）、１０４は両者の間で通信サービスを提供するためのネットワークである。クライアント側コンピュータ１０１では各種のWWW用ブラウザが動作し、サーバ側コンピュータ１０２および１０３ではWWWサービスを提供する各種デーモンプログラムが動作し、ネットワーク１０４を通してユーザに提供するための情報が蓄積されている。１０２と１０３の違いは、１０２は１０１の側のユーザ情報を管理しており、１０３は１０１の側のユーザ情報を管理していない事である。各コンピュータ１０１，１０２および１０３はネットワーク１０４によって接続されている。

【００１５】図２に、本発明のより詳細なシステム構成の一実施例を示す。同図において、クライアント側コンピュータ１０１中の、２０１がWWWサービスの提供を受けるための各種ブラウザ、２０２が該コンピュータ１０１を制御するための各種オペレーティングシステムであり、また、サーバ側コンピュータ１０２および１０３中の、２０３がWWWサービスにおいてユーザに提供するための情報（ハイパーテキストなど）の蓄積部、４０１が対話管理可能なWWWサービスを提供するためのサービス制御部（デーモン）、４０２が対話管理を行うために必要な情報を蓄積する対話記憶部、２０５が該コンピュータ１０２，１０３を制御するための各種オペレーティングシステムである。コンピュータ１０２は、クライアント側コンピュータ１０１を用いるユーザのユーザ情報を管理しているホームサーバであり、コンピュータ１０３はクライアント側コンピュータ１０１のホームサーバではないサーバコンピュータである。

【００１６】図３は、コンピュータ１０２，１０３内のサービス制御部（デーモン）４０１の詳細構成を示した

ので、６０１がアクセス制御部、６０２が対話識別部、６０３が通信処理部である。

【００１７】クライアント側コンピュータ１０１のブラウザ２０１からは、該コンピュータ１０１の入力装置から入力されたユーザからのＵＲＬに従い、ネットワーク１０４上のWWWサーバに情報取得要求が発行される。情報取得要求を受けたサーバ側コンピュータ１０２または１０３のサービス制御部４０１では、アクセス制御部６０１において情報提供およびアクセスの可否の判定を行い、対話識別部６０２においてはアクセスが許可されたユーザへの対話ＩＤの発行および対話ＩＤごとにユーザのアクセス情報の管理を行い、通信処理部６０３によって蓄積装置２０３内の情報をユーザに転送する。

【００１８】図４は、本発明によるクライアントとサーバ間のシーケンスの一例を示したものである。ここで、サーバＡとサーバＢは提携関係にあるとする。

【００１９】始めのユーザＡに対する例では、クライアント（ブラウザ）においてユーザＡからのＵＲＬの入力によりサーバＡへ情報取得要求（１回目のアクセス）を行い、対話ＩＤ取得要求付き初期画面を取得する。次にクライアントでは、ユーザＡの操作により対話ＩＤ取得要求付き情報取得要求（２回目のアクセス）をサーバＡへ行う。サーバＡはクライアントからの情報取得要求が情報提供条件を満たしていれば（例えば、ユーザ名とパスワードの一致などで、この例ではユーザＡの情報がサーバＡにおいて管理されている）、対話ＩＤを発行し、対話記憶部４０２に対話ＩＤを記憶し、ユーザからの要求のあったハイパーテキスト（これには次の情報取得要求が付いている）に対話ＩＤを付加して出力する。この例では、次の情報取得要求の宛先がサーバＢ内のハイパーテキストであり、サーバＡで発行された対話ＩＤが付加された情報取得要求をサーバＢに発行する（３回目のアクセス）。対話ＩＤ付き情報取得要求を受け付けたサーバＢは、対話ＩＤを解析し、対話ＩＤ発行元のサーバＡへ対話ＩＤの照会とユーザ情報の取得要求を発行する。サーバＡでは、サーバＢからの問合わせに対して、対話記憶部４０２を検索して対話ＩＤの認証を行い、サーバＢへ認証結果およびシステム内（例えばＯＳへの問合わせ）のユーザ情報を返送する。サーバＢ、ではサーバＡから送信されて来た認証結果およびユーザ情報に基づき、サーバＢ内の情報のユーザＡへの提供の可否を判定する。この例では、ユーザＡへの情報提供を認めたため、サーバＢは自情報蓄積部２０３内のハイパーテキストをユーザＡに出力する。

【００２０】次のサーバＢをホームサーバとするユーザＢに対する例では、クライアント（ブラウザ）においてユーザＢからのＵＲＬの入力によりサーバＡへ情報取得要求（１回目のアクセス）を行い、対話ＩＤ取得要求付き初期画面を取得する。次にクライアントでは、ユーザＢの操作により対話ＩＤ取得要求付き情報取得要求（２回目のアクセス）をサーバＡへ行う。しかし、この例では、ユーザＢの情報がサーバＡにおいて管理されておらず、ユーザＢは一連のアクセスの過程においてホームサーバにおける認証を行っていない（サーバＢが発行した対話ＩＤがない）為に、サーバＡにおいてアクセスが拒否される。

【００２１】図５は、対話ＩＤ付き情報取得要求の実施例の一つとして、対話ＩＤ付きＵＲＬの一例を示たものである。初期画面を得るための始めのアクセスにおいて用いられる一回目のアクセスのＵＲＬは従来のWWWと同様である。２回目のアクセスにおいて、このＵＲＬにＩＤ取得要求を付加している。３回目以降のアクセスにおいては、各種情報取得要求の他に発行元サーバを明記した対話ＩＤを付加してサーバにアクセスを行う。そして、この対話ＩＤが他のサーバに対しても継承される。

【００２２】図６は、サーバ側コンピュータにおけるサービス制御部４０１の動作のフローチャートを示したものである。図６中、破線で囲った部分がアクセス制御部６０１と対話識別部６０２の動作、それ以外は通信処理部６０３の動作である。

【００２３】まず、ステップ１００２において、サービス制御部への入力がクライアントからの情報取得要求であるか、他のサーバからの対話ＩＤの問い合わせかを判別する。他のサーバからの対話ＩＤの問い合わせの場合は、ステップ１００３～１００６の処理を行い、判定結果とユーザ情報を問い合わせのあったサーバへ返送する。クライアントからの情報取得要求である場合は、初回アクセスであるのか、ＩＤ取得要求であるのか、対話ＩＤ付き情報取得要求であるのか、ステップ１００７および１００９で判別する。初回アクセスの場合は、ステップ１００８でＩＤ取得要求付き初期画面を返送するための処理を行う。ＩＤ取得要求の場合は、ＩＤ取得要求と共に送信されてくるユーザ情報に基づき対話ＩＤ発行の可否をステップ１０１０において判別し、対話ＩＤ発行を許可する場合には、ステップ１０１１～１０１４の処理を行ってユーザに情報を提供し、許可しない場合は、ステップ１０１５でアクセス拒否のメッセージを出力する。対話ＩＤ付き情報取得要求の場合は、ステップ１０１６で対話ＩＤの抽出、ステップ１０１７で該対話ＩＤのチェックを行う。そして、対話ＩＤが自分自身が発行したものである場合は、ステップ１０１８～１０２０の処理に従いユーザに情報を提供し、他サーバの発行した対話ＩＤの場合は、ステップ１０２１で対話ＩＤで識別されるサーバへ対話ＩＤの問い合わせを行い、ステップ１０２２で判定結果とユーザ情報を取得した後、ステップ１０２３でアクセスの可否をチェックし、アクセスを許可する場合はステップ１０２４，１０２５でユーザに情報を提供し、その以外の対話ＩＤの場合は不正な対話ＩＤとみなし、ステップ１０２６でアクセス拒否の処理を行う。

7

【００２４】

【発明の効果】以上説明したように、本発明によれば、先の特願平７－１２５３８７号において導入した一連のアクセスに対する識別子を、異なるサーバ間で継承して有効にする事により、サーバにまたがった一連のアクセスにおいて一貫性を持ったアクセス制御ができるようになる。

【図面の簡単な説明】

【図１】本発明で対象とする通信サービスを提供するためのシステム構成の一例である。

【図２】本発明によるシステム構成の一実施例の詳細図である。

【図３】図２のサーバ内のサービス制御部の詳細図である。

【図４】本発明におけるクライアントとサーバ間のシーケンスの一例である。

【図５】本発明における対話ＩＤ付き情報取得要求を実現するためのＵＲＬの一例である。

【図６】本発明におけるサーバのサービス制御部のフローチャートの一例である。

【図７】従来のWWWサービスを提供するためのシステム構成の一例である。

8

【図８】従来のWWWサービスのサーバとクライアントにおけるシーケンスの一例である。

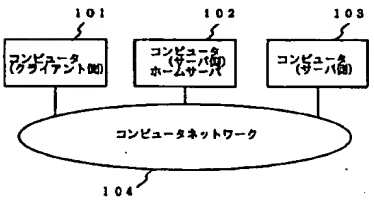
【図９】本出願人が先に提案したシステム構成の一例である。

【図１０】図９のシステム構成のサーバとクライアントにおけるシーケンスの一例である。

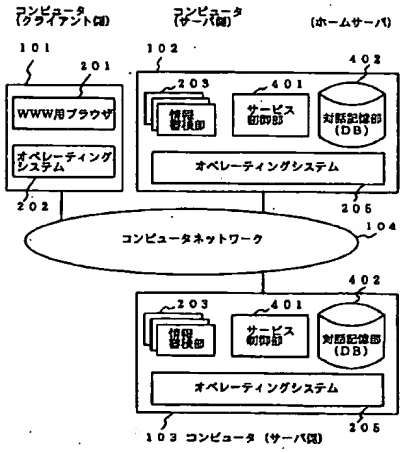
【符号の説明】

１０１　被サービス提供側コンピュータ
１０２，１０３　サービス提供側コンピュータ
１０４　ネットワーク
２０１　WWWブラウザ
２０２　オペレーティングシステム
２０３　情報蓄積部
２０４　WWWデーモン
２０５　オペレーティングシステム
４０１　サービス制御部
４０２　対話記憶部
６０１　アクセス制御部
６０２　対話識別部
６０３　通信処理部

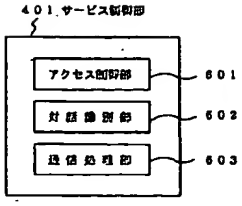
【図１】



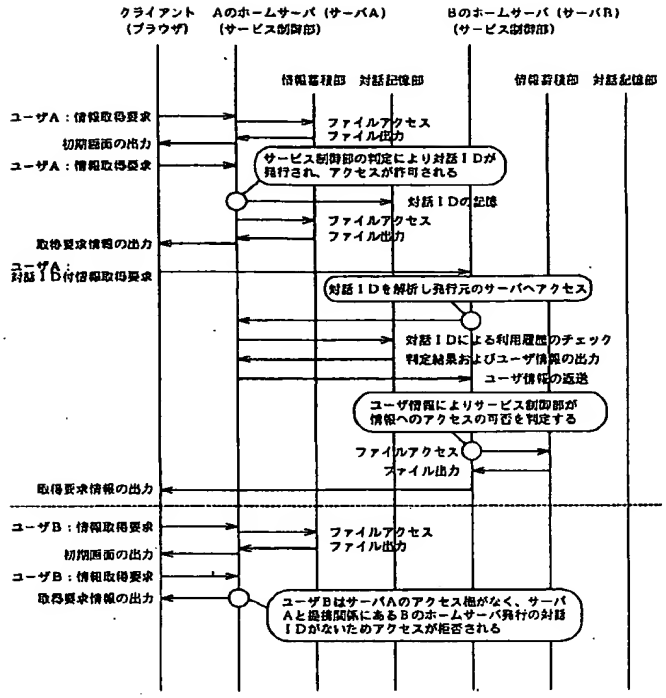
【図２】



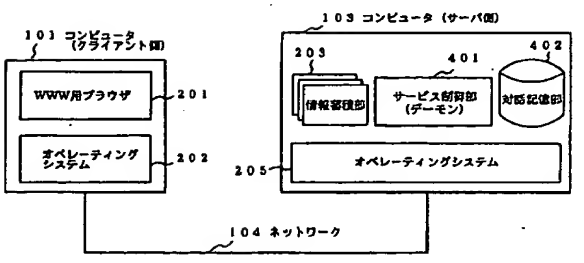
【図３】



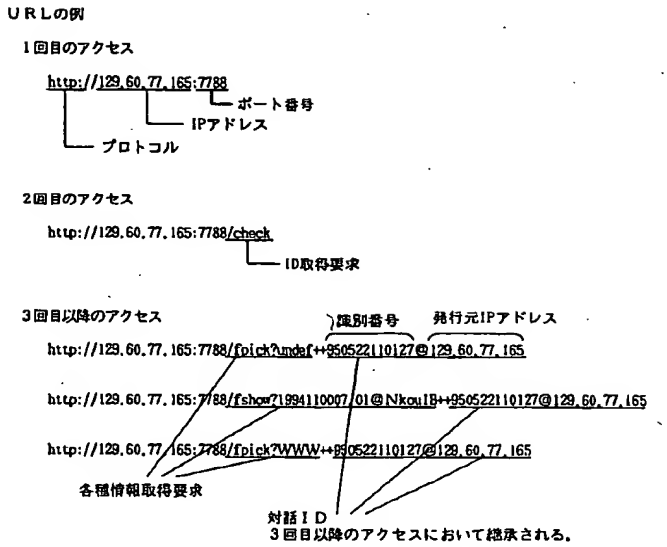
【図４】


クライアント（ブラウザ）
Aのホームサーバ（サーバA）（サービス制御部）
Bのホームサーバ（サーバB）（サービス制御部）
情報蓄積部
対話記憶部
情報蓄積部
対話記憶部
ユーザA：情報取得要求
ファイルアクセス
ファイル出力
初期画面の出力
ユーザA：情報取得要求
サービス制御部の判定により対話ＩＤが発行され、アクセスが許可される
対話ＩＤの記憶
ファイルアクセス
ファイル出力
取得要求情報の出力
ユーザA：対話ＩＤ付情報取得要求
対話ＩＤを解析し発行元のサーバへアクセス
対話ＩＤによる利用履歴のチェック
判定結果およびユーザ情報の出力
ユーザ情報の返送
ユーザ情報によりサービス制御部が情報へのアクセスの可否を判定する
ファイルアクセス
ファイル出力
取得要求情報の出力
ユーザＢ：情報取得要求
ファイルアクセス
ファイル出力
初期画面の出力
ユーザＢ：情報取得要求
取得要求情報の出力
ユーザＢはサーバAのアクセス権がなく、サーバAと提携関係にあるＢのホームサーバ発行の対話ＩＤがないためアクセスが拒否される

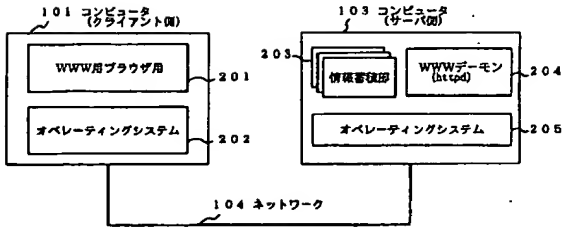
【図９】


101 コンピュータ（クライアント側）
WWW用ブラウザ
201
オペレーティングシステム
202
103 コンピュータ（サーバ側）
203
401
402
情報蓄積部
サービス制御部（デーモン）
対話記憶部
オペレーティングシステム
205
104 ネットワーク

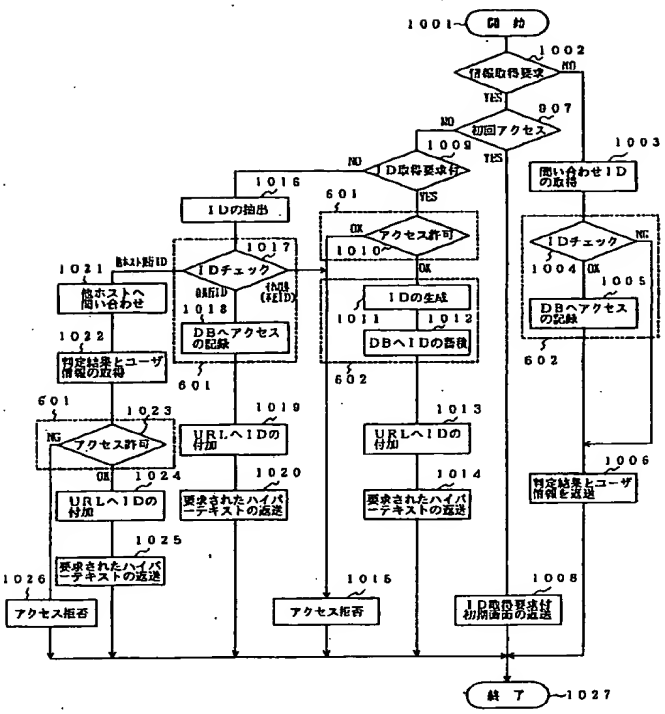
【図５】


ＵＲＬの例
１回目のアクセス
http://129.60.77.165:7788
ポート番号
IPアドレス
プロトコル
２回目のアクセス
http://129.60.77.165:7788/check
ID取得要求
３回目以降のアクセス
識別番号
発行元IPアドレス
http://129.60.77.165:7788/fpick?undef++9505221l0127@129.60.77.165
http://129.60.77.165:7788/fshow?1994110007.01@NkouIB++9505221l0127@129.60.77.165
http://129.60.77.165:7788/fpick?WWW++9505221l0127@129.60.77.165
各種情報取得要求
対話ＩＤ
３回目以降のアクセスにおいて継承される。

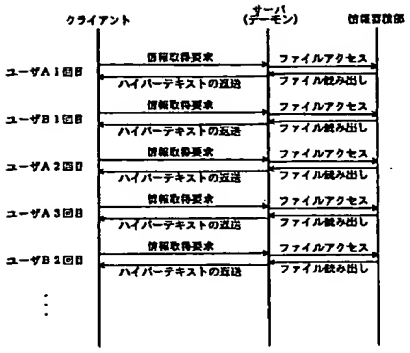
【図７】


101 コンピュータ (クライアント側)
WWW用ブラウザ用
201
オペレーティングシステム
202
103 コンピュータ (サーバ側)
203
情報蓄積部
WWWデーモン (httpd)
204
オペレーティングシステム
205
104 ネットワーク

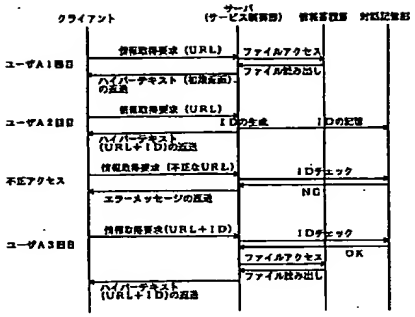
【図6】


開始
1001
情報取得要求
1002
NO
YES
初回アクセス
1007
NO
YES
ID取得要求有
1009
NO
YES
問い合わせID
の取得
1003
IDの抽出
1016
601
アクセス許可
1010
OK
NG
IDチェック
1004
OK
NG
DBへアクセス
の記録
1005
602
IDチェック
1017
1021
触れト時ID
他ホストへ
問い合わせ
1018
DBへアクセス
の記録
601
1022
判定結果とユーザ
情報の取得
601
1023
アクセス許可
NG
OK
1024
URLへIDの
付加
1025
要求されたハイパ
ーテキストの送
1026
アクセス拒否
1019
URLへIDの
付加
1020
要求されたハイパ
ーテキストの送
IDの生成
1011
1012
DBへIDの登録
602
1013
URLへIDの
付加
1014
要求されたハイパ
ーテキストの送
1015
判定結果とユーザ
情報を送
1006
IDを取得要求付
初期画面の送
1008
終了
1027

【図８】


クライアント
サーバ
(デーモン)
情報蓄積部
ユーザA１回目
ユーザB１回目
ユーザA２回目
ユーザA３回目
ユーザB２回目
情報取得要求
ハイパーテキストの返送
ファイルアクセス
ファイル読み出し

【図１０】


クライアント
サーバ
(サービス制御部)
情報蓄積部
対応記憶部
ユーザA１回目
ユーザA２回目
不正アクセス
ユーザA３回目
情報取得要求（URL）
ファイルアクセス
ファイル読み出し
ハイパーテキスト（転送定義）の返送
IDの生成
IDの記憶
ハイパーテキスト（URL＋ID）の返送
情報取得要求（不正なURL）
IDチェック
NG
エラーメッセージの返送
情報取得要求(URL＋ID)
OK
ハイパーテキスト（URL＋ID）の返送